(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-252773
(P2005-252773A)
(43)公開日　平成17年9月15日(2005.9.15)

(51)Int.Cl.[7]		F I			テーマコード（参考）
H04L	9/14	H04L	9/00	641	5C025
H04L	9/08	H04N	5/44	A	5C063
H04N	5/44	H04N	7/16	Z	5C064
H04N	7/08	H04N	7/08	Z	5J104
H04N	7/081	H04L	9/00	601C	

審査請求 未請求　請求項の数 65　OL　（全 24 頁）　最終頁に続く

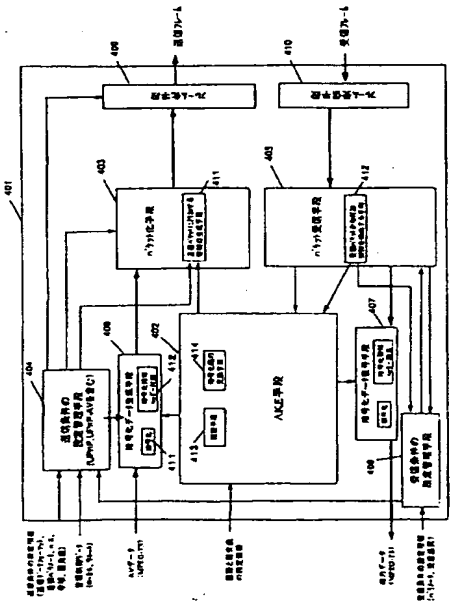
(21)出願番号　特願2004-61961 (P2004-61961)
(22)出願日　平成16年3月5日 (2004.3.5)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100097445
弁理士　岩橋　文雄
(74)代理人　100103355
弁理士　坂口　智康
(74)代理人　100109667
弁理士　内藤　浩樹
(72)発明者　森岡　芳宏
大阪府門真市大字門真１００６番地　松下電器産業株式会社内
(72)発明者　綾木　靖
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

最終頁に続く

(54)【発明の名称】パケット送信機器

(57)【要約】
【課題】デジタル放送やＤＶＤディスクなどの著作権保護されたＭＰＥＧなどのＡＶコンテンツを、そのフォーマット情報やコピー制御情報を継承しつつ、ＩＰネットワーク上で秘匿性を守って伝送する手段を実現する。
【解決手段】パケット送信手段は、ＡＶデータと非ＡＶデータとをそれぞれ入力するデータ入力手段と、前記データ入力手段の出力を入力し、規定の送受信条件により「暗号化または暗号化情報ヘッダー付加の実行を行う」暗号化データ生成手段と、パケットヘッダー付加手段とを具備するパケット送受信手段において、前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、または、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加のいずれかを行う制御手段とを具備する。
【選択図】図４



【特許請求の範囲】
【請求項１】
パケット送信機器とパケット受信機器の間でデータのパケット通信を行なうパケット送受信システムにおけるパケット送信機器であって、
前記パケット送信機器は、
ＡＶデータと非ＡＶデータとをそれぞれ入力するデータ入力手段と、
前記データ入力手段の出力を入力し、規定の送受信条件により、暗号化または暗号化情報ヘッダー付加の実行を行う暗号化データ生成手段と、
パケットヘッダー付加手段とを具備し、
前記暗号化データ生成手段は、認証処理を含む制御手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、前記非ＡＶデータは前記ＡＶデータのコピー制御情報、およびフォーマット情報を含み、前記コピー制御情報およびフォーマット情報より、前記暗号化手段において暗号化の制御、または、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加を行うか行わないかの制御の少なくとも一方の制御を行う手段とを具備するパケット送信機器。
【請求項２】
前記暗号化データ生成手段内の前記暗号化手段は、暗号化に際して暗号化鍵を使用し、前記パケット送信機器と前記パケット受信機器が規定の条件を具備していることを検証し認証が行われた後に暗号化鍵が前記パケット送信機器と前記パケット受信機器で共有され、規定の伝送条件により前記暗号化鍵が更新されることを特徴とする請求項１記載のパケット送信機器。
【請求項３】
前記暗号化鍵は、前記パケット送信機器が持っている暗号化鍵生成用の元データと、複数モードを持つ暗号化制御情報に対応した複数の暗号化鍵をメモリ空間に保持し、送信の暗号化モードが決定の後、前記複数の暗号化鍵よりその暗号化モードに応じた暗号化鍵を選択して暗号化手段の暗号化鍵を設定し、暗号化を行うことを特徴とする請求項２記載のパケット送信機器。
【請求項４】
前記暗号化鍵生成用の元データは、機器またはデバイスの証明書、機器固有情報、外部から設定する鍵作成データの少なくとも一部の情報を含むことを特徴とする請求項３記載のパケット送信機器。
【請求項５】
前記制御手段において、前記ＡＶデータのコピー制御情報が、コピーフリーの場合には、前記ＡＶデータのフォーマット情報を変更しないで前記ＡＶデータに付加して前記パケット送信機器から前記パケット受信機器に伝送を行ない、また、前記ＡＶデータのコピー制御情報がコピーフリー以外の場合には、前記ＡＶデータのフォーマット情報を変更した後、前記ＡＶデータを暗号化したデータに付加して前記パケット送信機器から前記パケット受信機器に伝送を行なうことを特徴とする請求項２記載のパケット送信機器。
【請求項６】
前記ＡＶデータのフォーマット情報は、ＭＩＭＥタイプ、ファイルタイプ、または拡張子のいずれかを含むことを特徴とする請求項５記載のパケット送信機器。
【請求項７】
前記認証処理を含む制御手段において認証を実行するモードは、前記データ入力手段より入力される前記ＡＶデータまたは前記非ＡＶデータが含んでいる制御情報により決定されることを特徴とする請求項１記載のパケット送信機器。
【請求項８】
前記外部より入力される制御情報または認証用のＴＣＰポート情報は、コンテンツ毎にアクセス位置を指定するＵＲＩ、または、Ｑｕｅｒｙにより拡張されたＵＲＩ情報とにより与えられることを特徴とする請求項７記載のパケット送信機器。
【請求項９】

前記外部より入力される制御情報または認証用のＴＣＰポート情報は、コンテンツ毎にアクセス位置を指定するＵＲＩで要求されたコンテンツの情報の返信時に与えることを特徴とする請求項７記載のパケット送信機器。
【請求項１０】
前記認証手段において認証を実行するモードは、
前記外部より入力される制御情報および前記入力ＡＶデータの双方により決定することを特徴とする請求項３記載のパケット送信機器。
【請求項１１】
前記前記暗号化情報ヘッダーは、暗号化モード情報と暗号化ペイロード長の少なくとも１つを含んでいることを特徴とする請求項１から１０のいずれかに記載のパケット送信機器。
【請求項１２】
前記暗号化情報ヘッダーは、前記ＡＶデータがコピーフリーコンテンツを放送する放送チャネルを受信したコンテンツの場合には付加しない、
また、前記ＡＶデータが一定期間でもコピーフリーでないコンテンツを放送する放送チャネルを受信したコンテンツの場合には付加する、また、前記ＡＶデータが蓄積メディアよりコピーフリータイトルのコンテンツを再生した場合には付加しない、
また、前記ＡＶデータが蓄積メディアよりコピーフリーでないタイトルのコンテンツを再生した場合には付加する、ことを特徴とする請求項１１記載のパケット送信機器。
【請求項１３】
前記コピーフリーコンテンツを放送する放送チャネルは、アナログ放送であるＶＨＦ、ＵＨＦ、またはＢＳアナログ放送の放送チャネルであることを特徴とする請求項１２記載のパケット送信機器。
【請求項１４】
前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルのコピー制御情報は、コピーネバー、コピーワンジェネレーション、およびＥＰＮフラグ付きコピーフリーのうち少なくとも１つのモードを含んでいることを特徴とする請求項１２記載のパケット送信機器。
【請求項１５】
前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルは、デジタル放送であるＢＳデジタル放送、地上波デジタル放送、またはＣＳデジタル放送の放送チャネルであることを特徴とする請求項１２記載のパケット送信機器。
【請求項１６】
前記一定期間でもコピーフリーでないコンテンツを放送する放送チャネルの受信は、前記放送の配信を行う事業者との間での認証手段により正当な受信機器または受信ユーザであることを認証された場合に行われることを特徴とする請求項１５記載のパケット送信機器。
【請求項１７】
前記認証は、日本のデジタル衛星放送のＢ－ＣＡＳカード、または米国のＣＡＴＶ放送で使用されるＰＯＤカードなどのセキュリティモジュールによる認証であることを特徴とする請求項１６記載のパケット送信機器。
【請求項１８】
前記暗号化手段は前記暗号化情報ヘッダーを、前記ＡＶデータがフリーコンテンツの場合には付加しない、または、前記ＡＶコンテンツの意味のあるデータ単位毎に付加することを特徴とする請求項１から１０のいずれかに記載のパケット送信機器。
【請求項１９】
ＡＶデータと非ＡＶデータとをそれぞれのデータバッファに入力し、前記２つのバッファの出力は優先制御して前記パケットヘッダー付加手段に出力することを特徴とする請求項１から１８のいずれかに記載のパケット送信機器。
【請求項２０】

前記優先制御の方法は、前記非ＡＶデータが前記データバッファでオーバーフローしない様に制御しながら、前記ＡＶデータを前記データバッファから優先して出力することを特徴とする請求項１９記載のパケット送信機器。
【請求項２１】
前記前記パケットヘッダー付加手段に出力は、あらかじめ決められた間隔値に対して一定のゆらぎ幅を持った概略一定間隔毎に出力する様に、パケットシェーピングして出力することを特徴とする請求項１９記載のパケット送信機器。
【請求項２２】
前記暗号化鍵を共有するための認証と鍵交換方式は、ＤＴＣＰ方式であることを特徴とする請求項１から２１のいずれかに記載のパケット送信機器。
【請求項２３】
前記暗号化鍵のＩＤ情報または更新情報として整数値を前記暗号化情報ヘッダーまたはパケットヘッダーに付加することを特徴とする請求項２２記載のパケット送信機器。
【請求項２４】
パケットヘッダー付加手段から出力されるパケットをＨＴＴＰプロトコルで伝送する場合、ＨＴＴＰパケットのパケット毎に、前記整数値はランダム値または特定の規則に基づく更新値に更新することを特徴とする請求項２３記載のパケット送信機器。
【請求項２５】
パケットヘッダー付加手段から出力されるパケットをＨＴＴＰプロトコルで伝送する場合、ＴＣＰプロトコルが切断して再コネクションを張る毎に、前記整数値はランダム値または特定の規則に基づく更新値に更新することを特徴とする請求項２３記載のパケット送信機器。
【請求項２６】
前記暗号化モードの変化はＴＣＰプロトコルまたはＵＤＰプロトコルのポート番号の変化で検出して設定することを特徴とする請求項２２記載のパケット送信機器。
【請求項２７】
前記暗号化モードの情報をパケット内に持つことを特徴とする請求項２２記載のパケット送信機器。
【請求項２８】
前記ＡＶデータのパケット化は、ＲＴＰ、ＵＤＰ、ＩＰプロトコルで行うことを特徴とする請求項１から２７のいずれかに記載のパケット送信機器。
【請求項２９】
前記暗号化鍵の更新条件としては、あらかじめ決められた時間ごとに行うという条件も用いることを特徴とする請求項２８記載のパケット送信機器。
【請求項３０】
前記ＡＶデータのパケット化は、ハードウエアで行うことを特徴とする請求項２８記載のパケット送信機器。
【請求項３１】
マルチキャスト伝送の場合、前記暗号化上布ヘッダーを付加したパケットと付加しないパケットの両方を出力することを特徴とする請求項２８記載のパケット送信機器。
【請求項３２】
前記ＡＶデータを前記ＲＴＰ、ＵＤＰ、ＩＰプロトコルによるＩＰパケット化の前に、フォーワードエラーコレクション（ＦＥＣ）による誤り訂正を付加することを特徴とする請求項２８記載のパケット送信機器。
【請求項３３】
前記フォーワードエラーコレクション（ＦＥＣ）はリードソロモン方式またはパリティ方式であることを特徴とする請求項２８記載のパケット送信機器。
【請求項３４】
前記暗号化情報ヘッダーを付加する場合は、前期ＲＴＰプロトコルにおいて定義されているマーカービット（Ｍビット）を有効状態にアサートすることを特徴とする請求項２８記

載のパケット送信機器。
【請求項３５】
前記ＡＶデータのパケット化は、ＨＴＴＰ、ＴＣＰ、ＩＰプロトコルで行うことを特徴とする請求項１から２７のいずれかに記載のパケット送信機器。
【請求項３６】
前記暗号化鍵の更新条件としては、あらかじめ決められた時間ごとに行うという条件も用いることを特徴とする請求項３５記載のパケット送信機器。
【請求項３７】
前記認証モードでは前記ＨＴＴＰヘッダーに、認証モード情報を付加することを特徴とする請求項３５記載のパケット送信機器。
【請求項３８】
前記ＡＶデータのパケット化は、受信側からの制御によりＲＴＰまたはＨＴＴＰプロトコルで行うことを切替え制御することを特徴とする請求項１から３６記載のパケット送信機器。
【請求項３９】
前記ＡＶデータのパケット化は、受信側でのチャネル選択時には受信側からの制御によりＲＴＰプロトコルを用いて行ない、受信チャネルが確定した後にＨＴＴＰプロトコルを用いて行う様に切り替え制御することを特徴とする請求項３８記載のパケット送信機器。
【請求項４０】
前記ＡＶデータのパケット化は、受信側のＡＶデータ出力が表示ディスプレイに対して出力されており蓄積されない場合はＲＴＰを用い、また、受信側のＡＶデータ出力が記録メディアに蓄積される場合はＨＴＴＰを用いる様に、切替え制御することを特徴とする請求項３８記載のパケット送信機器。
【請求項４１】
前記ＡＶデータは、ＳＭＰＴＥ ２５９Ｍ規格で規定された非圧縮ＳＤ方式信号、または、ＳＭＦＴＥ ２９２Ｍ規格で規定された非圧縮ＨＤ形式、または、ＩＥＣ６１８８３規格で規定されたＩＥＥＥ１３９４によるＤＶまたはデジタル放送のＭＰＥＧ－ＴＳの伝送ストリーム形式、または、ＤＶＢ規格Ａ０１０で規定されたＤＶＢ－ＡＳＩによるＭＰＥＧ－ＴＳ形式、または、ＭＰＥＧ－ＰＥＳ，ＭＰＥＧ－ＥＳ、ＭＰＥＧ４、ＩＳＯ／ＩＥＣ Ｈ．２６４の内のいずれか一つのデータストリーム形式を含むことを特徴とする請求項２８から４０のいずれかに記載のパケット送信機器。
【請求項４２】
前記ＡＶデータを構成するデータブロックに時間情報を付加し、１つ以上の時間情報付データブロックをまとめてＲＴＰまたはＨＴＴＰ上にマッピングすることを特徴とする請求項４１記載のパケット送信機器。
【請求項４３】
前記時間情報としては、送信側の規定条件によりタイムスタンプ又は定型値データを選択して用いることを特徴とする請求項４２記載のパケット送信機器。
【請求項４４】
ＭＩＭＥタイプ、ファイルタイプ、または拡張子のいずれかを含む前記ＡＶデータのフォーマット情報をタイムスタンプ付加の判別条件に用いて、前記送信側でタイムスタンプが付加できる場合には、前記タイムスタンプを用いることを特徴とする請求項４３記載のパケット送信機器。
【請求項４５】
前記ＡＶデータは、ＭＰＥＧ－ＴＳであることを特徴とする請求項４２記載のパケット送信機器。
【請求項４６】
前記各ＴＳパケットに付加するタイムスタンプのクロックはＭＰＥＧのシステムクロック周波数に等しいことを特徴とする請求項４３記載のパケット送信機器。
【請求項４７】

前記ＴＳパケットに付加された時間情報がタイムスタンプの場合、ＭＰＥＧ－ＴＳのネットワーク伝送により前記各ＴＳパケットに重畳されたジッターを受信側のシステムクロック値と前記書くTSパケットのタイムスタンプの差分を一定にすることで伝送された前記書くTSパケットの伝送ジッターを除去して、受信側で前記ＴＳパケットに含まれるＰＣＲを用いてＭＰＥＧシステムクロックの再生を行うことを特徴とする請求項４６記載のパケット送信機器。

【請求項４８】

前記ＴＳパケットに付加された時間情報が定型値データの場合、受信したＭＰＥＧ－ＴＳは送信時の時刻情報を用いないでＭＰＥＧデコードを行うことを特徴とする請求項４６記載のパケット送信機器。

【請求項４９】

Ｎを２以上の整数とした場合、ＵＤＰプロトコルまたはＴＣＰプロトコルのＮ個のポートを用いて、Ｎ個のフォーマットのＡＶデータをそれぞれのポート毎に割り当てて伝送することを特徴とする請求項４１記載のパケット送信機器。

【請求項５０】

ＵＤＰプロトコルまたはＴＣＰプロトコルの単一のポートを用いて、複数のフォーマットのＡＶデータを多重して伝送することを特徴とする請求項４１記載のパケット送信機器。

【請求項５１】

Ｎを２以上の整数、また、ＭをＮより大きい整数とした場合、ＵＤＰプロトコルまたはＴＣＰプロトコルのＭ個のポートを用いて、Ｎ個のフォーマットのＡＶデータを単一または多重してＭ個のポートに割り当てて伝送することを特徴とする請求項４１記載のパケット送信機器。

【請求項５２】

複数のＡＶデータを同時に伝送する場合、高データレートのＡＶデータはＵＤＰプロトコルで伝送し、低データレートのＡＶデータはＴＣＰプロトコルで伝送することを特徴とする請求項４１記載のパケット送信機器。

【請求項５３】

複数のＡＶデータを同時に伝送する場合、高データレートのＡＶデータより、低データレートのＡＶデータを優先して伝送することを特徴とする請求項４１記載のパケット送信機器。

【請求項５４】

前記ＡＶデータの伝送範囲を制限することを特徴とする請求項１から５３のいずれかに記載のパケット送信機器。

【請求項５５】

前記ＡＶデータの伝送範囲の制限は、ＩＰプロトコルのＴＴＬ（Ｔｉｍｅ ｔｏ Ｌｉｖｅ）の値を用いて制限することを特徴とする請求項５４記載のパケット送信機器。

【請求項５６】

前期前記ＡＶデータの伝送範囲を制限は、ＩＰパケットのＲＴＴ（Ｒｏｕｎｄ Ｔｒｉｐ Ｔｉｍｅ）の値を用いて制限することを特徴とする請求項５４記載のパケット送信機器。

【請求項５７】

前記ＡＶデータの伝送範囲を制限は、ＭＡＣ層のヘッダー情報により制限することを特徴とする請求項５４記載のパケット送信機器。

【請求項５８】

前記ＩＰパケットのパケットサイズは前記送信手段と前記受信手段の中間に位置するＩＰネットワークのパスＭＴＵサイズ以下に設定することを特徴とする請求項１から５７のいずれかに記載のパケット送信機器。

【請求項５９】

前記ＩＰパケットの伝送は、ＩＥＥＥ ８０２．３で規定された伝送方法により行われることを特徴とする請求項１から５７のいずれかに記載のパケット送信機器。

【請求項６０】
前記ＩＰパケットの伝送は、ＩＥＥＥ　８０２．１１で規定された伝送方法により行われることを特徴とする請求項１から５７のいずれかに記載のパケット送信機器。
【請求項６１】
前記ＩＥＥＥ　８０２．１１の使用において、ＷＥＰまたはＷＰＡまたはその他のネットワーク接続制限手段を用いることを特徴とする請求項６０記載のパケット送信機器。
【請求項６２】
前記ＩＰパケットの伝送は、ＩＥＥＥ　８０２．１Ｑにより規定された伝送方法により行われることを特徴とする請求項１から５７のいずれかに記載のパケット送信機器。
【請求項６３】
前記ＩＰパケットの伝送は、ＩＰバージョン４、または、ＩＰバージョン６を使用して行われることを特徴とする請求項１から５７記載のパケット送信機器。
【請求項６４】
前記ＩＰバージョン４を用いる場合、ＴＯＳフィールドを用いて優先制御を行なうことを特徴とする請求項６３記載のパケット送信機器。
【請求項６５】
前記ＩＰバージョン６を用いる場合、Ｐｒｉｏｒｉｔｙフィールドを用いて優先制御を行なうことを特徴とする請求項６３記載のパケット送信機器。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ＩＥＥＥ　８０２．３などのイーサネット（Ｒ）（有線ＬＡＮ）やＩＥＥＥ　８０２．１１などの無線ＬＡＮなどを用いて、暗号化されたＡＶストリームをＩＰパケット化して高品質に送信するパケット送信機器に関する。
【背景技術】
【０００２】
従来、一般家庭において、ＩＥＥＥ　１３９４を用いて、ＩＥＣ　６１８８３－４で規定された方式に基づきＭＰＥＧ－ＴＳ信号の暗号化伝送が行なわれている。ＭＰＥＧ－ＴＳなどＡＶデータを暗号化して伝送する方式の一例として、ＤＴＣＰ（Digital Transmission Content Protection）方式が規定されている。ＤＴＣＰは、ＩＥＥＥ　１３９４やＵＳＢなどの伝送メディア上のコンテンツ保護技術である。ＤＴＣＰ方式は、ＤＴＬＡ(Digital Transmission Licencing Administrator)で規格化された方式であり、http://www.dtcp.com、http://www.dtcp.com/data/dtcp_tut.pdf、http://www.dtcp.com/data/wp_spec.pdfや、書籍「ＩＥＥＥ１３９４、ＡＶ機器への応用」、高田信司監修、日刊工業新聞社、「第８章、コピープロテクション」（133～149ページ）で説明されている。
【０００３】
図１２は、ＤＴＣＰ方式を用いたＭＰＥＧ－ＴＳのＩＥＥＥ　１３９４での伝送の一例である。ＤＴＣＰ方式では、送信側をソース（１８０１）、受信側をシンク（１８０２）と呼び、暗号化したＭＰＥＧ－ＴＳなどのコンテンツをソース（１８０１）からネットワーク（１８０３）を介して、シンク（１８０２）へ伝送している。図１２に、補足情報として、ソース機器およびシンク機器の例を併記する。
【０００４】
次に、図１３を用いて、ＤＴＣＰ方式における従来のパケット通信手段の概略を説明する。図１３は図１２のソース（１８０１）、およびシンク（１８０２）の構成の概略図である。まず、ＤＴＣＰ方式に準拠した認証と鍵交換（Authentification and Key Exchange、ＡＫＥと略する）が行なわれる。ＡＫＥ手段（１９０１）に対して、その認証と鍵交換設定情報が入力され、この情報がパケット化手段（１９０２）により規定のヘッダーを付加されパケット化され、ネットワーク（１９０７）に出力される。ここで、パケット化手段（１９０２）は送信条件設定手段（１９０３）により決定された送信パラメータにより、入力データのパケット化および送信を行なう。受信側では、ネットワーク（１９０７

）より入力する信号がパケット受信手段（１９０４）でパケットヘッダーなどの識別によりフィルタリングされ、ＡＫＥ手段（１９０１）に入力される。これにより送信側（ソース）のＡＫＥ手段と、受信側（シンク）のＡＫＥ手段がネットワーク（１８０３、１９０７）を介してお互いにメッセージの通信ができる。すなわち、ＤＴＣＰ方式の手順に従い、認証と鍵交換を実行する。

【０００５】

送信側（ソース）と、受信側（シンク）で認証と鍵交換が成立すれば、次に、ＡＶデータの伝送を行なう。ソースでは、ＭＰＥＧ－ＴＳ信号を暗号化データ生成手段（１９０５）に入力して、ＭＰＥＧ－ＴＳ信号を暗号化した後、この暗号化されたＭＰＥＧ－ＴＳ信号をパケット化手段（１９０２）に入力し、ネットワーク（１９０７）に出力する。シンクでは、ネットワーク（１９０７）より入力する信号がパケット受信手段（１９０４）でパケットヘッダーなどの識別によりフィルタリングされ、暗号化データ復号手段（１９０６）に入力され、復号されＭＰＥＧ－ＴＳ信号が出力される。

【０００６】

次に、図１４を用い上記手順を補足説明する。図１４において、ソースとシンク間はＩＥＥＥ　１３９４で接続されている。まず、ソース側でコンテンツの送信要求が発生する。そして、ソースからシンクへ暗号化されたコンテンツおよびコンテンツの保護モード情報が送信される。シンクは、コンテンツのコピー保護情報の解析を行い、完全認証もしくは制限付き認証のどちらの認証方式を用いるかを決定し、認証要求をソースに送る。ソースとシンクはＤＴＣＰ所定の処理により認証鍵（Kauth）の共有を図る。そして、ソースは認証鍵を用いて交換鍵(Kx)を暗号化してシンクに送り、シンクで交換鍵（Ｋｘ）が復号される。ソースでは暗号鍵(Kc)を時間的に変化させるために、時間的に変化するシード情報(Nc)を生成し、シンクに送信する。ソースでは、交換鍵(Nx)とシード情報(Nc)より暗号化鍵(Kx)を生成して、ＭＰＥＧ－ＴＳをこの暗号化鍵を用いて暗号化手段で暗号化してシンクに送信する。シンクはシード情報を受信し交換鍵とシード情報情報より復号鍵を復元する。シンクではこの復号鍵を用いて暗号化されたＭＰＥＧ－ＴＳ信号を復号する。

【０００７】

図１５は、図１２においてＭＰＥＧ－ＴＳ信号を伝送する場合のＩＥＥＥ　１３９４アイソクロナスパケットの一例である。このパケットは、４バイト（３２ビット）のヘッダー、４バイト（３２ビット）のヘッダーＣＲＣ、２２４バイトのデータフィールド、４バイト（３２ニット）のトレイラによって構成されている。暗号化されて伝送されるのは２２４バイトのデータフィールドを構成するＣＩＰヘッダーとＴＳ信号のうち、ＴＳ信号のみで、他のデータは暗号化されない。ここで、ＤＴＣＰ方式固有の情報は、コピー保護情報である２ビットのＥＭＩ（Encription Mode Indicator）、および１ビットのシード情報Ｏ／Ｅ（Odd/Even）であり、これらは上記３２ビットのヘッダー内に存在するため暗号化されずに伝送される。

【特許文献１】特開２００４－５６７７６号公報

【非特許文献１】「ＩＥＥＥ１３９４、ＡＶ機器への応用」、高田信司監修、日刊工業新聞社、「第８章、コピープロテクション」（133～149ページ）

【発明の開示】

【発明が解決しようとする課題】

【０００８】

しかしながら、上記従来の構成では以下のような問題点を有していた。従来のＤＴＣＰ方式はＩＥＥＥ　１３９４において、アイソクロナスパケットを用いて伝送するためＭＰＥＧ－ＴＳ信号のリアルタイム伝送ができるが、インターネットの標準プロトコルであるＩＰプロトコルを用いて、イーサネット（Ｒ）（ＩＥＥＥ　８０２．３）、無線ＬＡＮ（ＩＥＥＥ　８０２．１１）や、その他のＩＰパケットを伝送可能なネットワークで伝送ができないという大きな問題点がある。すなわち、ＩＰプロトコルを介して論理的に接続された送信機器と受信機器の間を、暗号化によりコンテンツの機密性や著作権の保護を行なった状態でＭＰＥＧ－ＴＳ信号などＡＶストリームを伝送できないという大きな問題点が

あある。

【課題を解決するための手段】

【０００９】

上記課題を解決するために、本願第１の発明は、ＡＶデータと非ＡＶデータとをそれぞれ入力するデータ入力手段と、前記データ入力手段の出力を入力し、規定の送受信条件、すなわち、AVデータのコピー制御情報、およびフォーマット情報により、暗号化または暗号化情報ヘッダー付加の実行を行う暗号化データ生成手段と、パケットヘッダー付加手段とを具備するパケット送信機器において、前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、または、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加を行うか行わないかの少なく共いずれか一方を制御する手段とを具備する。これにより、ＭＰＥＧ－ＴＳ信号などのＡＶストリームを外部から与えられる一定規則による送信条件に従い暗号化モードを決め、さらに暗号化情報ヘッダーを付加を決めることにより、送受信機器間での信号の互換性を確保しながら、ＡＶストリームの秘匿性を保つこと、すなわち、コンテンツの著作権を保護することが可能となる。

【００１０】

本願第２の発明は、第１の発明における暗号化手段におけるＡＶデータ伝送中の鍵更新において、複数の暗号化鍵から１つの暗号化鍵を選択して暗号化処理を高速実行するために、暗号化鍵はパケット送信機器が持っている暗号化鍵生成用の元データと、複数モードを持つ暗号化制御情報に対応した複数の暗号化鍵をメモリ空間に保持し、送信の暗号化モードが決定の後、複数の暗号化鍵よりその暗号化モードに応じた暗号化鍵を選択して暗号化手段の暗号化鍵を設定し、暗号化を行う。これらの構成により、高速なＡＶデータを伝送しながら、複数の暗号化鍵から１つの暗号化鍵を選択して鍵更新を高速に行いながら、暗号化処理を高速実行することが可能となる。

本願第３の発明は、第１の発明における暗号化データ生成手段において、外部入力されるＡＶストリームのコピー制御情報（ＣＣＩ）に従うより、ＭＩＭＥ－ＴＹＰＥなどＡＶデータのフォーマット情報を暗号化データ仕様のフォーマットに変更をした後、暗号化伝送する。さらに、ＡＶストリームのオリジナルのフォーマット情報をＵＰｎＰ－ＡＶ方式や独自の通信方式を利用して別のデータにマッピングして、送信側から受信側に伝送する。これらの構成により、ＡＶデータのフォーマット情報を変更して暗号化伝送しながら、受信側でＡＶデータのオリジナルのフォーマット情報を復元することが可能となる。

本願第４の発明は、第１の発明において、ＡＶデータのパケット化は、受信側からの制御により、ＲＴＰ／ＵＤＰまたはＨＴＴＰ／ＴＣＰプロトコルの切替え制御を、きめ細かく、かつ映像の途切れなくスムースに行う。たとえば、ＡＶデータのパケット化は、受信側から送信側におけるＴＶチューナのチャネル選択や、受信側でＨＤＤがＤＶＤディスクに録画されたＡＶコンテンツの選択を行う場合には、伝送遅延の小さいＲＴＰ／ＵＤＰプロトコルを用い、ＴＶチューナのチャネル選択や録画されたＡＶコンテンツの選択を速く行うことができる。また、これらの視聴コンテンツ選択が終了した後は、ＨＴＴＰ／ＴＣＰプロトコルを用い、ＲＴＰ／ＵＤＰよりもパケット落ちに対してＴＣＰでの再送機能を持つＨＴＴＰ／ＴＣＰ方式を用いて高画質なコンテンツ視聴を行う。これらの構成により、切替え制御することにより受信側でコンテンツ選択をする場合は低遅延でユーザに遅延を感じさせない軽快な操作が可能となり、また、視聴コンテンツ選択が終了した後はパケットロスなどによる信号欠落が補償された高品質なＡＶコンテンツの伝送が可能となる。

本願第５の発明は、第１の発明において、ＡＶデータを構成するデータブロックに、タイムスタンプまたは提携データから構成される時間情報を付加し、時間情報を付加した付データブロックを１つ以上まとめてＲＴＰパケットのペイロード部またはＨＴＴＰパケットのペイロード部にマッピングする。これにより、ＴＳパケットにタイムスタンプや特定情報を付加できるので、受信側でＭＰＥＧ－ＴＳのデコードをタイムスタンプを用いて行うか、タイムスタンプを用いないで用いるかをきめ細かく制御することが可能となる。

【発明の効果】

【００１１】
本願第１の発明によれば、以下のような効果を有する。すなわち、本願第１の発明によるパケット送信手段は、ＡＶデータと非ＡＶデータとをそれぞれ入力するデータ入力手段と、前記データ入力手段の出力を入力し、規定の送受信条件、すなわち、AVデータのコピー制御情報、およびフォーマット情報により「暗号化または暗号化情報ヘッダー付加の実行を行う」暗号化データ生成手段と、パケットヘッダー付加手段とを具備するパケット送受信手段において、前記暗号化データ生成手段は認証手段と暗号化手段と暗号化情報ヘッダー付加手段を具備し、前記規定の送受信条件により前記暗号化手段において暗号化を実行するかしないか、または、前記暗号化情報ヘッダー付加手段において暗号化情報ヘッダー付加を行うか行わないかの少なく共いずれか一方を制御する手段とを具備する。これにより、ＭＰＥＧ－ＴＳ信号などのＡＶストリームを外部から与えられる一定規則による送信条件に従い暗号化モードを決め、さらに暗号化情報ヘッダーを付加を決めることにより、送受信機器間での信号の互換性を確保しながら、ＡＶストリームの秘匿性を保つこと、すなわち、コンテンツの著作権を保護することが可能となる。
本願第２の発明によれば、以下のような効果を有する。すなわち、本願第２の発明によるパケット送信手段は、第１の発明における暗号化手段におけるＡＶデータ伝送中の鍵更新において、複数の暗号化鍵から１つの暗号化鍵を選択して暗号化処理を高速実行するために、暗号化鍵は送信手段が持っている暗号化鍵生成用の元データと、複数モードを持つ暗号化制御情報に対応した複数の暗号化鍵をメモリ空間に保持し、送信の暗号化モードが決定の後、複数の暗号化鍵よりその暗号化モードに応じた暗号化鍵を選択して暗号化手段の暗号化鍵を設定し、暗号化を行う。これらの構成により、高速なＡＶデータを伝送しながら、複数の暗号化鍵から１つの暗号化鍵を選択して鍵更新を高速に行いながら、暗号化処理を高速実行することが可能となる。
本願第３の発明によれば、以下のような効果を有する。本願第３の発明は、第１の発明における暗号化データ生成手段において、外部入力されるＡＶストリームのコピー制御情報（ＣＣＩ）に従うより、ＭＩＭＥ－ＴＹＰＥなどＡＶデータのフォーマット情報を暗号化データ仕様のフォーマットに変更をした後、暗号化伝送する。さらに、ＡＶストリームのオリジナルのフォーマット情報をＵＰｎＰ－ＡＶ方式や独自の通信方式を利用して別のデータにマッピングして、送信側から受信側に伝送する。これらの構成により、ＡＶデータのフォーマット情報を変更して暗号化伝送しながら、受信側でＡＶデータのオリジナルのフォーマット情報を復元することが可能となる。
本願第４の発明によれば、以下のような効果を有する。本願第４の発明は、第１の発明において、ＡＶデータのパケット化は、受信側からの制御により、ＲＴＰ／ＵＤＰまたはＨＴＴＰ／ＴＣＰプロトコルの切替え制御を、きめ細かく、かつ映像の途切れなくスムースに行う。たとえば、ＡＶデータのパケット化は、受信側から送信側におけるＴＶチューナのチャネル選択や、受信側でＨＤＤがＤＶＤディスクに録画されたＡＶコンテンツの選択を行う場合には、伝送遅延の小さいＲＴＰ／ＵＤＰプロトコルを用い、ＴＶチューナのチャネル選択や録画されたＡＶコンテンツの選択を速く行うことができる。また、これらの視聴コンテンツ選択が終了した後は、ＨＴＴＰ／ＴＣＰプロトコルを用い、ＲＴＰ／ＵＤＰよりもパケット落ちに対してＴＣＰでの再送機能を持つＨＴＴＰ／ＴＣＰ方式を用いて高画質なコンテンツ視聴を行う。これらの構成により、切替え制御することにより受信側でコンテンツ選択をする場合は低遅延でユーザに遅延を感じさせない軽快な操作が可能となり、また、視聴コンテンツ選択が終了した後はパケットロスなどによる信号欠落が補償された高品質なＡＶコンテンツの伝送が可能となる。
本願第５の発明によれば、以下のような効果を有する。すなわち、本願第５の発明は、第１の発明において、ＡＶデータを構成するデータブロックに、タイムスタンプまたは提携データから構成される時間情報を付加し、時間情報を付加した付データブロックを１つ以上まとめてＲＴＰパケットのペイロード部またはＨＴＴＰパケットのペイロード部にマッピングする。これにより、ＴＳパケットにタイムスタンプや特定情報を付加できるので、受信側でＭＰＥＧ－ＴＳのデコードをタイムスタンプを用いて行うか、タイムスタンプを

用いないで用いるかをきめ細かく制御することが可能となる。
また、本願第１から第５までの発明によれば、ネットワークを用いたＡＶコンテンツの伝送に関して、ネットワーク上でのデータ盗聴を防止し、安全性の高いデータ伝送を実現する。これにより、伝送路にインターネットなど公衆網を使用した場合においても、リアルタイム伝送される優先データ（ＡＶデータコンテンツ）の盗聴、漏洩を防止することができる。また、インターネット等で伝送されるＡＶデータの販売、課金が可能となり、安全性の高いＢ－Ｂ、Ｂ－Ｃのコンテンツ販売流通が可能となる。
また、本願第２から第６５での発明によれば、ＡＶコンテンツをハードウエアで伝送処理する場合にも、一般のデータパケットは従来通りＣＰＵを用いてソフトウェア処理を行える。よって、ソフトウェアの追加により管理情報や制御情報などデータを一般データとして伝送させることができる。これらのデータ量は優先データであるＡＶデータに比べて非常に少ないので、マイコンなど安価なマイクロプロセッサーで実現可能となり低コストで実現することができる。なお、高負荷かつ高伝送レート優先パケットのプロトコル処理にも高価なＣＰＵや大規模メモリを必要としないので、これらの点からも低コストで高機能な装置を提供できるという大きなメリットがある。
【発明を実施するための最良の形態】
【００１２】
まず最初に本願発明の位置付けを明確にするために適用されるシステム例の概略について説明する。図１は本願発明を適用するシステムの一例である。
図１において、パケット送信機器（１０１）およびパケット受信機器（１０３）は、本願第１，２，３、４および５の発明実施部である（以下、本願発明部）。１０１は送信機器、１０２はルータ、１０３は受信機器である。送信機器（１０１）には、送受信条件の設定情報、認証と鍵交換の設定情報、入力ストリーム（ＭＰＥＧ－ＴＳなどコンテンツ）が入力され、以下の手順１から３に基づき、通信が実行される。
手順１）送受信パラメータの設定を行なう。
（1-1）送受信機器のＭＡＣアドレス、ＩＰアドレス、ＴＣＰ／ＵＤＰポート番号等を設定。
（1-2）送信信号フォーマットの種別、帯域を設定。ＱｏＳエージェントとして動作する送信機器（１０１）と受信機器（１０３）、ＱｏＳマネージャとして動作するルータ（１０２）との間でＩＥＥＥ　８０２．１Ｑ（ＶＬＡＮ）規格を用いたネットワークの運用に関する設定を実施。
（1-3）優先度の設定（ＩＥＥＥ　８０２．１Ｑ／ｐによる運用）
手順２）認証と鍵交換：
（2-1）認証と鍵交換を行なう。たとえば、ＤＴＣＰ方式を用いることもできる。
手順３）ストリーム伝送：
（3-1）送信機器と受信機器間での暗号化されたストリームコンテンツ(MPEG-TS)の伝送
なお、コンテンツの入力信号として、例ではＭＰＥＧ－ＴＳを使用しているが、これに限らず本発明で用いる入力コンテンツの適用範囲としては、ＭＰＥＧ１／２／４などＭＰＥＧ－ＴＳストリーム（ＩＳＯ／ＩＥＣ　１３８１８）、ＤＶ（ＩＥＣ　６１８３４、ＩＥＣ　６１８８３）、ＳＭＰＴＥ　３１４Ｍ（ＤＶ－ｂａｓｅｄ）、ＳＭＰＴＥ　２５９Ｍ（ＳＤＩ）、ＳＭＰＴＥ　３０５Ｍ（ＳＤＴＩ）、ＳＭＰＴＥ　２９２Ｍ（ＨＤ－ＳＤＩ）等で規格化されているストリームなお、一般的なＡＶコンテンツも適用可能である。さらに、本発明で用いる入力データの適用範囲として、データのファイル転送にも適用可能である。ファイル転送の場合、送受信端末の処理能力と送受信端末間の伝播遅延時間の関係により、データ転送速度がコンテンツストリームの通常再生データレートよりも大きくなるなどの条件化において、リアルタイムより高速のコンテンツ伝送も可能である。
次に、上記手順２の認証と鍵交換に関して補足説明する。図２において、送信機器と受信機器間はＩＰネットワークにより接続されている。まず、送信機器から受信機器へコンテンツのコピー保護情報を含んだコンテンツの保護モード情報が送信される。受信機器は、コンテンツのコピー保護情報の解析を行い、使用する認証方式を決定して認証要求を送信

機器に送る。これらの処理を通して送信機器と受信機器は認証鍵を共有する。次に、送信機器は認証鍵を用いて交換鍵を暗号化して受信機器に送り、受信機器で交換鍵が復号される。送信機器では暗号鍵を時間的に変化させるために、時間的に変化する鍵変更情報を生成し、受信機器に送信する。送信機器では、交換鍵と鍵変更情報より暗号化鍵を生成して、ＭＰＥＧ－ＴＳをこの暗号化鍵を用いて暗号化手段で暗号化して受信機器に送信する。受信機器は受信した鍵変更情報を交換鍵より復号鍵を復元する。受信機器ではこの復号鍵を用いて暗号化されたＭＰＥＧ－ＴＳ信号を復号する。

図３は本方式をイーサネット（Ｒ）を用い２階建ての家庭に適用した場合の一例である。図３において、３０１は１階のネットワーク構成、３０２は２階のネットワーク構成である。３０３は１階に設置されインターネットと接続されるルータ、３０４は２階に設置されているスイッチングハブである。３０４はルータ（３０３）とスイッチングハブ（３０４）を接続するイーサネット（Ｒ）ネットワークである。家庭内の全てのイーサネット（Ｒ）ネットワークの帯域は１００Ｍｂｐｓである。１階のネットワーク構成の詳細としては、ルータ（３０３）にはテレビ（ＴＶ）、パソコン（ＰＣ）、ＤＶＤレコーダが１００Ｍｂｐｓのイーサネット（Ｒ）で接続され、また、エアコン、冷蔵庫がＥＣＨＯＮＥＴで接続されている。また、２階では、スイッチングハブ（３０４）にテレビ（ＴＶ）、パソコン（ＰＣ）、ＤＶＤレコーダが１００Ｍｂｐｓのイーサネット（Ｒ）で接続され、また、エアコンがＥＣＨＯＮＥＴで接続されている。なお、ＥＣＨＯＮＥＴは「エコーネットコンソーシアム」（http://www.echonet.gr.jp/）で開発されている伝送方式である。

図３において、パソコン（ＰＣ）、ＤＶＤレコーダ、ルータ（３０１）およびスイッチングハブ（３０４）は、ＩＥＥＥ　８０２．１Ｑ（ＶＬＡＮ）に対応している。すなわち、ルータ（３０１）およびスイッチングハブ（３０４）において、各ポートのデータレートが全て同じ（例えば１００Ｍｂｐｓ）場合、特定ポートへ出力されるデータ帯域の合計がそのポートの伝送レートの規格値または実力値を超えない限り、入力ポートへ入力されたデータはルータ（あるいは、スイッチングハブ）内部で失われず全て出力ポートに出力される。スイッチングハブでは、たとえば８個の入力ポートにデータが同時に入力されても、それぞれのデータの出力ポートが異なっていれば、それぞれのデータはハブ内部のバッファで競合しないでスイッチングされて出力ポートより出力されるため、入力データはパケット落ちすることなく全て出力ポートに出力される。

図３において、家庭内の全てのイーサネット（Ｒ）の帯域が１００Ｍｂｐｓであるため、１階と２階間のネットワーク３０５の帯域も１００Ｍｂｐｓである。１階と２階の複数の機器間で複数のデータが流れる場合、各データに対する帯域制限がない場合、このネットワーク３０５上を流れるデータのデータレート合計が１００Ｍｂｐｓを超える可能性があり、ＭＰＥＧ－ＴＳの映像アプリなどリアルタイム伝送が必要なストリームが途切れる可能性がある。この場合、リアルタイム伝送が必要なストリームが途切れない様にするには、伝送データに対して優先制御が必要である。端末だけでなく、ルータやスイッチングハブにおいて、後述するストリーム伝送やファイル転送の速度制限機構などを導入することにより解決できる。たとえば、ＭＰＥＧ－ＴＳストリームの伝送優先度をファイル転送データの伝送優先度よりも高くすると、１階と２階のＰＣ間でのファイル転送をバックグラウンドで行いながら、同時に、１階および２階のＤＶＤレコーダ、ＰＣ，ＴＶの間でＭＰＥＧ－ＴＳを暗号化してリアルタイムで伝送することが可能となる。

前述したルータ、またはスイッチングハブにおける伝送速度制限機構は、データ流入制御により実現できる。すなわち、ルータ（あるいは、スイッチングハブ）の入力データキューにおいて優先度の高いデータと低いデータを比較して、優先度の高いデータを優先して出力することにより実現できる。この優先制御方式に用いるバッファ制御ルールとしては、ラウンドロビン方式、流体フェアスケジューリング方式、重み付けフェアスケジューリング方式自己同期フェアスケジューリング方式ＷＦＦＱ方式、仮想時計スケジューリング方式、クラス別スケジューリング方式などがある。これらのスケジューリング方式に関する情報は、戸田巌著、「ネットワークＱｏＳ技術」、平成１３年５月２５日（第１版）、オーム社刊の第１２章などに記述されている。

（実施の形態１）

本願第１の発明について説明する。図４は本願第１の発明のパケット送受信手段（機器）に関するブロック図である。４０１はＡＫＥ手段を用いた暗号化によるパケット送受信手段である。ＡＫＥ手段（４０２）に対してＡＫＥ設定情報を入力され、このＡＫＥ設定情報に関連した情報、たとえばコピー保護情報と暗号化鍵変更情報、がパケット化手段（４０３）に入力され、ＴＣＰ／ＩＰプロトコルのヘッダーを付加され、さらに、フレーム化手段４０９においてＭＡＣヘッダーが付加されイーサネット（Ｒ）フレームに変換し、送信フレームとしてネットワークに出力される。ここで、パケット化手段（４０３）は送信条件設定手段（４０４）により決定された送信パラメータにより、入力データのパケット化および送信を行なう。なお、送信条件設定管理手段（４０４）には、ＡＶデータのフォーマット情報は、ＭＩＭＥタイプ、ファイルタイプ、または拡張子のいずれかを含む送信データのフォーマット種別、送信先アドレスやポート番号の情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段（ローカル）と受信手段（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータが入力され、パケット化手段（４０３）およびフレーム化手段（４０９）で生成するヘッダーやペイロードデータなどを設定する。

【００１３】

ここで、送信先アドレスやポート番号の情報などの設定はＵＰｎＰフォーラムが規定しているUPnP、デバイスアーキテクチャー（たとえば、DA ver.1.0）を参照して利用する。また、ＵＰｎＰ以外のＷＥＢブラウザーを利用したアプリケーションや独自のアプリケーションで設定してもよい。

また、ＡＶデータのフォーマット情報は、ＭＩＭＥタイプ、ファイルタイプ、または拡張子のいずれかを含む送信データのフォーマット種別などより構成され、コピー制御情報（ＣＣＩ、Ｃｏｐｙ　Ｃｏｎｔｒｏｌ　Ｉｎｆｏｒｍａｔｉｏｎ）などとともに、ＵＰｎＰフォーラムの規定しているＵＰｎＰ－ＡＶ仕様を参照して設定する。また、ＵＰｎＰ－ＡＶで規定する仕様以外のＷＥＢブラウザーを利用したアプリケーションや独自のアプリケーションで設定してもよい。

受信側では、ネットワークより入力する信号がフレーム受信手段（４１０）でＭＡＣヘッダーを元にフィルタリンングされ、ＩＰパケットとしてパケット受信手段（４０５）に入力される。パケット受信手段（４０５）ではＩＰパケットヘッダーなどの識別によりフィルタリングを行い、ＡＫＥ手段（４０２）に入力される。これにより送信側のＡＫＥ手段と、受信側のＡＫＥ手段がネットワークを介して接続されるので、通信プロトコルを介してお互いにメッセージの交換ができる。すなわち、ＡＫＥ手段の設定手順に従い、認証と鍵交換を実行することができる。

【００１４】

送信側と、受信側で認証と鍵交換が成立すれば、暗号化したＡＶデータを送信する。送信条件設定手段（４０４）は、この時、ＡＶデータのコピー制御情報、およびフォーマット情報により暗号化モードの設定、または、暗号化情報ヘッダー付加の実行の少なく共いずれか一方の動作を、暗号化データ生成手段（４０６）、およびパケット化手段（４０３）に対して制御する。

送信側では、ＭＰＥＧ－ＴＳ信号を暗号化手段（４０６）に入力して、ＭＰＥＧ－ＴＳ信号を暗号化した後、この暗号化されたＭＰＥＧ－ＴＳ信号をパケット化手段（４０３）に入力し、ＴＣＰ／ＩＰプロトコルのヘッダーを付加する。さらに、フレーム化手段４０９において、８０２．１Ｑ（ＶＬＡＮ）方式を用いて、ＭＡＣヘッダーを付加しイーサネット（Ｒ）フレームに変換して、送信フレームとしてネットワークに出力する。ここで、ＭＡＣヘッダー内のＴＣＩ（Tag Controal Informaition）内のＰｒｉｏｒｉｔｙ（ユーザ優先度）を高く設定することにより、ネットワーク伝送の優先度を一般のデータよりも高くすることができる。

受信側では、ネットワークより入力する信号がフレーム受信手段（４１０）でＭＡＣヘッ

ダーを元にフィルタリングされ、ＩＰパケットとしてパケット受信手段（４０５）に入力される。パケット受信手段（４０５）でパケットヘッダーなどの識別によりフィルタリングされ、復号手段（４０７）に入力され、復号されたＭＰＥＧ－ＴＳ信号が出力される。

【００１５】

なお、送信条件設定手段（４０４）には、受信状況を送信側にフィードバックするためのデータが入力され、パケット化手段（４０３）およびフレーム化手段（４０９）で生成するヘッダーおよびペイロードデータを設定する。

【００１６】

次に、図５のプロトコルスタックを用い上記手順を補足説明する。図５の送信側において、まず送信側から受信側へ暗号化されたコンテンツおよびコンテンツの保護モード情報が送信される。受信側は、コンテンツのコピー保護情報の解析を行い、認証方式を決定し、認証要求を送信機器に送る。次に、乱数を発生させ、この乱数を所定の関数に入力し、交換鍵を作成する。交換鍵の情報を所定の関数に入力し、認証鍵を生成する。受信側でも所定の処理により認証鍵の共有を図る。なお、ここで用いる暗号化情報としては、たとえば、送信側の独自情報（機器ＩＤ、機器の認証情報、マックアドレスなど）、秘密鍵、公開鍵、外部から与えられた情報などを１つ以上組み合わせて生成した情報であり、ＤＥＳ方式やＡＥＳ方式など暗号化強度の強い暗号化方式を用いることにより強固な暗号化が可能である。そして、送信側は認証鍵を用いて交換鍵を暗号化して受信側に送り、受信側で交換鍵が復号される。また、交換鍵と初期鍵更新情報を所定の関数に入力し、暗号化鍵を生成する。なお、送信側では暗号鍵を時間的に変化させるために、時間的に変化する鍵更新報を生成し、受信側に送信する。コンテンツであるＭＰＥＧ－ＴＳは暗号化鍵により暗号化される。そして暗号化されたＭＰＥＧ－ＴＳは、１つ以上のＴＳパケットを単位として前述したＥＭＩなどの暗号化モード情報や、鍵生成の元情報となる数値情報と結合して、伝送ＡＶデータペイロードとしてＨＴＴＰやＲＴＰのパケットペイロードとしてマッピングされる。さらにこのＨＴＴＰまたはＲＴＰパケットは、ＴＣＰまたはＵＤＰプロトコルにマッピングされ、次にＩＰパケットのデータペイロードとして使用され、ＩＰパケットが生成される。さらにこのＩＰパケットはＭＡＣフレームのペイロードデータとして使用され、イーサネット（Ｒ）ＭＡＣフレームが生成される。なお、ＭＡＣとしてはイーサネット（Ｒ）であるＩＥＥＥ　８０２．３だけでなく、無線ＬＡＮ規格のＩＥＥＥ　８０２．１１のＭＡＣにも適用できる。

【００１７】

さて、イーサネット（Ｒ）ＭＡＣフレームは、イーサネット（Ｒ）上を送信側から受信側へ伝送される。受信側で所定の手順に従って復号鍵を生成する。そして、受信したイーサネット（Ｒ）ＭＡＣフレームからＩＰパケットがフィルタリングされる。さらにＩＰパケットからＴＣＰ（またはＵＤＰ）パケットが抜き出される。そして、ＴＣＰ（またはＵＤＰ）パケットからＡＶデータが抜き出され、交換鍵と鍵変更情報より復元された復号鍵により、ＭＰＥＧ－ＴＳ（コンテンツ）が復号され出力される。

【００１８】

以上、ＭＰＥＧ－ＴＳ信号などのＡＶストリームを送信機器で暗号化して、ＩＰパケットをネットワークにより伝送し、受信機器で元の信号に復号することが可能である。

なお、図３において、スイッチングハブを用いたネットワークトポロジーを工夫することにより、ストリーム伝送とファイル転送を共存させることができる。たとえば、１階と２階の間のネットワーク３０５の帯域を、従来の実施例で説明した１００Ｍｂｐｓから１Ｇｂｐｓに拡張することによって、１階と２階のＰＣ間でのファイル転送をバックグラウンドで行いながら、同時に、１階および２階のＤＶＤレコーダ、ＰＣ，ＴＶの間でＭＰＥＧ－ＴＳを暗号化してリアルタイムで伝送することができる。たとえば、市販されている１００Ｍｂｐｓのポートを８つ、１Ｇｂｐｓのポートを１つ持ったスイッチングハブを用い、１階と２階を結ぶネットワーク３０５に１Ｇｂｐｓのポートを接続し、残りの８ｃｈの１００Ｍｂｐｓのポートに ＴＶなどのＡＶ機器を接続する。１００Ｍｂｐｓのポートは８つなので、８つのポートのデータがそれぞれ最大１００Ｍｂｐｓで入力されて１Ｇ

ｂｐｓのポートに出力されたとしても、１００Ｍｂｐｓ×８ｃｈ＝８００Ｍｂｐｓと１Ｇｂｐｓより小さいため、８つのポートから入力されたデータはスイッチングハブ内部で失われず全て１Ｇｂｐｓのポートに出力される。よって、１階で発生したデータは全て２階に伝送することが可能である。また、逆に２階で発生したデータも全て１階に伝送することが可能である。以上の様に、スイッチングハブを用いる場合、ネットワークトポロジーを工夫することによりストリーム伝送とファイル転送を共存させることができる。

【００１９】

なお、ＡＫＥおよびＡＶデータの暗号化方式としてＤＴＣＰ方式を用いることができる。

（実施の形態２）

本願第２の発明について説明する。図６は本願第２の発明のブロック図である。図６においては、ＡＫＥ手段（４０２）、および複数の暗号化鍵の保持手段（６０２）以外は、図４と同様の構成である、よって以下では新規な部分について説明する。

【００２０】

本願第２の発明では、第１の発明における暗号化手段におけるＡＶデータ伝送中の鍵更新において、複数の暗号化鍵から１つの暗号化鍵を選択して暗号化処理を高速実行するために、暗号化鍵は送信手段が持っている暗号化鍵生成用の元データと、複数モードを持つ暗号化制御情報に対応した複数の暗号化鍵をメモリ空間に保持し、送信の暗号化モードが決定の後、複数の暗号化鍵よりその暗号化モードに応じた暗号化鍵を選択して暗号化手段の暗号化鍵を設定し、暗号化を行う。これらの構成により、高速なＡＶデータを伝送しながら、複数の暗号化鍵から１つの暗号化鍵を選択して鍵更新を高速に行いながら、暗号化処理を高速実行することが可能となる。

図６において、ＡＫＥ手段（４０２）に対してＡＫＥ設定情報を入力され、このＡＫＥ設定情報に関連した情報（たとえば、コピー制御情報と暗号化鍵変更情報）、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段（ローカル）と受信手段（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータがパケット化手段（４０３）に入力され、ＴＣＰ／ＩＰプロトコル処理をして、第１キュー手段（６０３）に入力される。

ここで、送信条件の設定管理手段（４０４）とＡＫＥ手段（４０２）は、それぞれ、暗号鍵を生成する情報を与え、ＡＫＥ手段（４０２）で複数の暗号化モード（ＥＭＩなど）に応じて１つ以上の暗号化鍵生成手段（６０１）を生成し、複数の暗号化鍵の保持手段（６０２）にセットする。伝送されるＡＶデータが暗号化データ生成手段（４０６）に入力されれば、そのＡＶデータのコピー制御情報に応じて、複数の暗号化鍵の保持手段（６０２）にセットされた複数の暗号化鍵より１つの暗号化鍵を選択する。この選択された暗号化鍵は、ＡＥＳ方式やＤＥＳ方式などの暗号化手段にセットにＡＶデータを暗号化し、パケット化手段（４０３）に出力する。ここで、暗号化鍵生成手段（６０１）はハードウエア、複数の暗号化鍵の保持手段（６０２）はソフトウエアのメモリ、暗号化手段はハードウエアの構成を使用することにより、高速で暗号化鍵の更新を行ないながらＡＶデータの送信が実現できる。

【００２１】

受信側の動作は第１の実施例と同様である。

（実施の形態３）

本願第３の発明について説明する。本願第３の発明は、第１の発明における暗号化データ生成手段において、外部入力されるＡＶストリームのコピー制御情報（ＣＣＩ）に従うより、ＭＩＭＥ－ＴＹＰＥなどＡＶデータのフォーマット情報を暗号化データ仕様のフォーマットに変更をした後、暗号化伝送する。さらに、ＡＶストリームのオリジナルのフォーマット情報をＵＰｎＰ－ＡＶ方式や独自の通信方式を利用して別のデータにマッピングして、送信側から受信側に伝送する。これらの構成により、ＡＶデータのフォーマット情報を変更して暗号化伝送しながら、受信側でＡＶデータのオリジナルのフォーマット情報

を復元することが可能となる。

【００２２】

図６は本願第３の発明のブロック図である。図６において、ＡＫＥ手段（４０２）に対してＡＫＥ設定情報を入力し、このＡＫＥ設定情報に関連した情報（たとえば、コピー保護情報と暗号化鍵変更情報）、および、送信データの種別、送信先アドレスやポート番号の情報、送信に用いるパス情報（ルーティング情報）、送信データの帯域、送信データの送信優先度などの送信条件の設定情報と、送信手段（ローカル）と受信手段（リモート）における機器の管理制御データと、受信状況を送信側にフィードバックするためのデータが第１のパケット化手段（７０１）に入力されプロセッサーを用いたソフトウエア処理でＴＣＰ／ＩＰプロトコル処理をされ、第１キュー手段（６０３）に入力される。送信条件の設定管理手段（４０４）には、ＡＶデータのフォーマット情報が入力されている。一方、ＡＶデータのフォーマット情報は、前述した暗号化モード（ＥＭＩなど）に応じて、そのフォーマット情報が書き換えられる。たとえば、暗号化しない場合はＡＶデータのフォーマット情報は、

ｖｉｄｅｏ／ｍｐｅｇのまま変更しない。また、暗号化する場合はＡＶデータのフォーマット情報は、ｖｉｄｅｏ／ｍｐｅｇからａｐｐｌｉｃａｔｉｏｎ／ｘ－ｄｔｃｐ１などに変更する。さらに、ｖｉｄｅｏ／ｍｐｅｇの付帯情報として、ｍｐｅｇ－ｐｓ、ｍｐｅｇ－ｔｓ、ＮＴＳＣやＰＡＬなどの情報をＡＶデータとしてではなく別データとして、ＵＰｎＰ－ＡＶや専用プロトコルなどを使用して送信側から受信側に伝送する。受信側では、受け取った情報から、元のＡＶデータのフォーマットを復元できる。これらのＭＩＭＥタイプはＩＥＴＦのＲＦＣ規格やＡＲＩＢ（電波産業界）の規格などに記述されている。ＡＲＩＢの規格に記述されている仕様としては、たとえば、

ａｐｐｌｉｃａｔｉｏｎ／ｘ－ａｒｉｂ－ｍｐｅｇ－ｔｓ

や

ａｐｐｌｉｃａｔｉｏｎ／ｘ－ａｒｉｂ－ｍｐｅｇ－ｔｔｓ

などがある。

（実施の形態４）

本願第４の発明について説明する。

本願第４の発明は、第１の発明において、ＡＶデータのパケット化は、受信側からの制御により、ＲＴＰ／ＵＤＰまたはＨＴＴＰ／ＴＣＰプロトコルの切替え制御を、きめ細かく、かつ映像の途切れなくスムースに行う。

図９は本願第４の発明のブロック図である。図９のパケット化手段（４０３）内の第１のパケット化手段（９０１）および第２のパケット化手段（９０２）、パケット受信手段（４０５）内の第１のパケット受信手段（９０３）および第２のパケット受信手段（９０４）を持つ。ここで第１のパケット化手段（９０１）はＲＴＰ方式、第２のパケット化手段（９０２）はＨＴＴＰ方式、第１のパケット受信手段（９０３）はＲＴＰ方式、また、第２のパケット受信手段（９０４）はＨＴＴＰ方式のパケット処理を行う。

ＡＶデータのパケット化は、受信側から送信側におけるＴＶチューナのチャネル選択や、受信側でＨＤＤがＤＶＤディスクに録画されたＡＶコンテンツの選択コマンドが出された場合には、第１のパケット化手段（９０１）および第１のパケット受信手段（９０３）を使用し、伝送遅延の小さいＲＴＰ方式で、ＴＶチューナのチャネル選択や録画されたＡＶコンテンツの選択を速く行う。また、これらの視聴コンテンツ選択が終了した後は、第２のパケット化手段（９０２）および第２のパケット受信手段（９０４）を使用し、ＨＴＴＰ／ＴＣＰプロトコルを用い、ＲＴＰ／ＵＤＰよりもパケット落ちに対してＴＣＰでの再送機能を持つＨＴＴＰ／ＴＣＰ方式を用いて高画質なコンテンツ視聴を行う。これらの構成により、切替え制御することにより受信側でコンテンツ選択をする場合は低遅延でユーザに遅延を感じさせない軽快な操作が可能となり、また、視聴コンテンツ選択が終了した後はパケットロスなどによる信号欠落が補償された高品質なＡＶコンテンツの伝送が可能となる。

（実施の形態５）

本願第５の発明について説明する。図１０は本願第５の発明のブロック図である。図１０においては、時間情報付加手段（１００１）、および時間情報判別手段（１００２）以外は、図９と同様の構成である、よって以下では新規な部分について説明する。

【００２３】

本願第５の発明は、第１の発明において、ＡＶデータを構成するデータブロックに、タイムスタンプまたは提携データから構成される時間情報を付加し、時間情報を付加した付データブロックを１つ以上まとめてＲＴＰパケットのペイロード部またはＨＴＴＰパケットのペイロード部にマッピングする。これにより、ＴＳパケットにタイムスタンプや特定情報を付加できるので、受信側でＭＰＥＧ－ＴＳのデコードをタイムスタンプを用いて行うか、タイムスタンプを用いないで用いるかをきめ細かく制御することが可能となる。

【００２４】

図１１は、ＭＰＥＧ－ＴＳをＩＰパケット化、さらにイーサネット（Ｒ）フレーム化して伝送する場合のパケット形式の一例である。１８８バイトのＭＰＥＧ－ＴＳに６バイトのタイムコード（ＴＣ）を付加して１９４バイトの単位を作る。ＴＣは４２ビットのタイムスタンプと６ビットのベースクロックＩＤ（ＢＣＩＤ）により構成される。ＢＣＩＤによりタイムスタンプの周波数情報を表すことができる。たとえば、（ケース１）ＢＣＩＤが０ｘ００の場合は、タイムスタンプの周波数情報はない、（ケース２）ＢＣＩＤが０ｚ０１の場合は、タイムスタンプの周波数情報としては２７ＭＨｚ（ＭＰＥＧ２のシステムクロック周波数）である、（ケース３）また、ＢＣＩＤが０ｘ０２の場合は、タイムスタンプの周波数情報としては９０ｋＨｚ（ＭＰＥＧ１で使用されるクロック周波数）である、（ケース４）ＢＣＩＤが０ｘ０３の場合は、タイムスタンプの周波数情報としては２４．５７６ＭＨｚ（ＩＥＥＥ　１３９４で使用されるクロック周波数）である。（ケース５）ＢＣＩＤが０ｘ０４の場合は、タイムスタンプの周波数情報としては１００ＭＨｚ（イーサネット（Ｒ）で使用される周波数）である、という様にＢＣＩＤでタイムスタンプの周波数情報を表すことができる。１９４バイト単位のデータを２つあわせて暗号化して、更に２バイトのＤＴＣＰ情報と合わせてＲＴＰプロトコルのペイロードとする。ここで、ＤＴＣＰ情報は、２ビットのＥＭＩと、１ビットのＯ／Ｅと１３ビットのReserved Dataにより構成される。ＲＴＰパケットはＵＤＰおよびＩＰプロトコルによりパケット化された後、イーサネット（Ｒ）フレーム化される。イーサネット（Ｒ）ヘッダとしては、図９に示す様に、標準的なイーサネット（Ｒ）ヘッダーとＩＥＥＥ　８０２．１Ｑ（ＶＬＡＮ）により拡張されたイーサネット（Ｒ）ヘッダーの両方をサポートする。なお、ＩＥＥＥ８０２．１Ｑ（ＶＬＡＮ）により拡張されたイーサネット（Ｒ）ヘッダーにおけるＴＣＩフィールドの中の３ビットのＰｒｉｏｒｉｔｙフラグにより、イーサネット（Ｒ）フレームの優先度を設定することができる。また、受信側でタイムスタンプのある状態とタイムスタンプのない状態を識別するには、ＵＰｎＰ－ＡＶや特定アプリーケーションで状態識別フラグを通知する構成をとってもよい。

【００２５】

また、ＭＰＥＧ－ＴＳにＡＲＩＢ－ＳＴＤ－Ｂ２１で規定された４バイトのタイムコード（ＴＣ）を付加して１９２バイトとしてもよい。この場合、前述した（ケース１）のＢＣＩＤが０ｘ００に相当する状態、すなわち、タイムスタンプの周波数情報のない状態として、オール１などある特定の値を定義してタイムスタンプのある状態とタイムスタンプのない状態を規定することができる。

【００２６】

受信側でタイムスタンプのある状態とタイムスタンプのない状態を識別するには、ＵＰｎＰ－ＡＶや特定アプリーケーションで状態識別フラグを通知する構成がとれる。また、４バイトデータとしてオール１などある特定の値の受信値から判別することもできる。

【００２７】

なお、上述した実施の形態１から５においては、一般のＩＰネットワークなどパケットの順序性が保証されていない通信網で伝送する場合には、パケットにシーケンス番号を付加して送信し、受信側でシーケンス番号を用いて順序性の保証を行ってもよい。この順序

性の保証は、ＯＳＩモデルの第４層以上、すなわち、ＲＴＰプロトコルやビデオ信号処理などで行なうことができる。

【００２８】

なお、送信側側でハードウエア処理され伝送されたＡＶ信号のパケットが、ネットワークでフラグメントされないため対策ができる。すなわち、送信側において、あらかじめアプリケーションレベルの処理で、通信網においてフラグメントされない最大サイズ（ＭＴＵ）を検査し、それ以下のパケットサイズで伝送すればよい。あるいは、ＲＦＣの規格では全ての端末は５７６バイトのサイズのＩＰパケットを扱えなければならないと規定されているので、ルータ等の多くのネットワーク機器はこれ以下のＩＰパケットではフラグメントが起こらない。したがってＩＰパケットのサイズが５７６バイト以下となるように、送信側側でハードウエア処理されるＡＶ信号のパケットサイズを調整すればよい。なお、送信側側でハードウエア処理されるＡＶ信号のパケットにフラグメントが起こらない場合は、受信したパケットがフラグメントされていれば全て一般パケットとして処理すればよい。なお、イーサネット（Ｒ）のＩＰパケットの最大値を越えた場合は送信端末でフラグメントしなければ行けないので、優先パケットのフラグメントを起こさせないためにはＩＰパケットの最大値以下でなければならないことは言うまでもない。

【００２９】

また、通信網においてフラグメントが起こる確率が非常に低い場合は、送信側側でハードウエア処理され伝送されたＡＶ信号のパケットのＩＰヘッダにフラグメント禁止のフラグを立てて伝送することにより、ルータがフラグメントせざるを得ない状態ではＩＰパケットを廃棄させることにより、受信端末のフラグメント処理負荷を軽減してもよい。この場合、非常に少数のパケットは損失となるが、受信側で誤り訂正あるいは誤り修整を行うことで通信品質を補償することができる。

さらに、実施の形態１から実施の形態６までは、通信網プロトコルとしてイーサネット（Ｒ）を例としたがこの限りではない。

【００３０】

また、ビデオ信号処理の例として、実施の形態１から５ではＭＰＥＧ－ＴＳを用いたが、これに限らず本発明で用いる入力データの適用範囲としては、ＭＰＥＧ１／２／４などＭＰＥＧ－ＴＳストリーム（ＩＳＯ／ＩＥＣ　１３８１８）、ＤＶ（ＩＥＣ　６１８３４、ＩＥＣ　６１８８３）、ＳＭＰＴＥ　３１４Ｍ（ＤＶ－ｂａｓｅｄ）、ＳＭＰＴＥ　２５９Ｍ（ＳＤＩ）、ＳＭＰＴＥ　３０５Ｍ（ＳＤＴＩ）、ＳＭＰＴＥ　２９２Ｍ（ＨＤ－ＳＤＩ）等で規格化されているストリームを含んだあらゆる映像、音声に関するストリームまでも適用可能である。映像や音声のデータレートは、ＣＢＲ（constant bit rate）に限るものではない。さらに、映像や音声だけでなく、一般のリアルタイムデータ、あるいは優先的に送受信を行うデータであればどのようなものでも本願発明から排除するものではない。

また、本発明で用いる入力データの適用範囲として、データのファイル転送にも適用可能である。ファイル転送の場合、送受信端末の処理能力と送受信端末間の伝播遅延時間の関係により、一定の条件化でリアルタイムより高速の伝送も可能である。

【図面の簡単な説明】

【００３１】

【図１】本願第１の発明を適用するシステムの一例を示す図

【図２】認証と鍵交換にＤＴＣＰ方式を適用する場合のコンテンツ伝送手順の説明図

【図３】イーサネット（Ｒ）を用いる一般家庭に適用した場合の一例の説明図

【図４】本願第１の発明のパケット送受信手段（機器）のブロック図

【図５】本願第１の発明のプロトコルスタックによる説明図

【図６】本願第２の発明のパケット送受信手段のブロック図

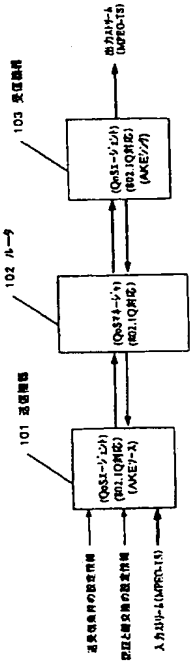
【図７】本願第３の発明のパケット送受信手段のブロック図

【図８】本願第３の発明のプロトコルスタックによる説明図

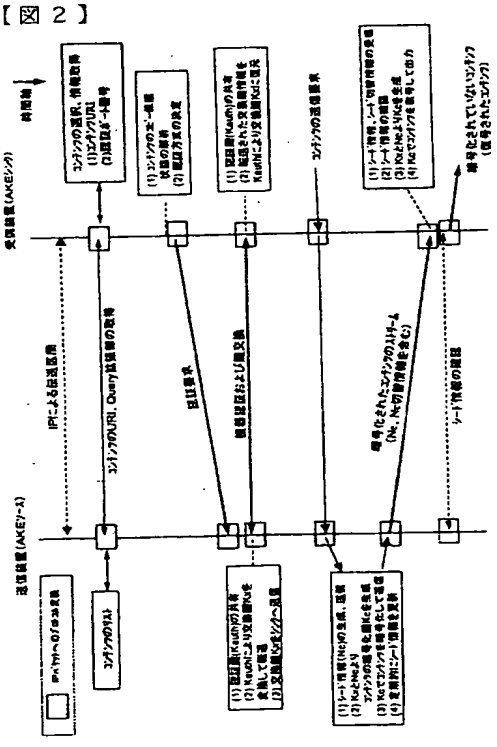
【図９】本願第４の発明のパケット送受信手段のブロック図

【図１０】本願第５の発明のパケット送受信手段のブロック図
【図１１】本願第５の発明におけるＭＰＥＧ－ＴＳのイーサネット（Ｒ）フレーム構成仕様の例を示す図
【図１２】ＤＴＣＰ方式を用いたＭＰＥＧ－ＴＳのＩＥＥＥ　１３９４での伝送の一例を示す図
【図１３】ＤＴＣＰ方式における従来のパケット通信手段の概略説明図
【図１４】ＩＥＥＥ　１３９４においてＤＴＣＰを用いた暗号化ストリーム伝送手順を示す図
【図１５】ＭＰＥＧ－ＴＳ信号を伝送する場合のＩＥＥＥ　１３９４アイソクロナスパケットの一例を示す図
【符号の説明】
【００３２】
１０１　パケット送信機器
１０２　ルータ
１０３　パケット受信機器
４０１　パケット送受信手段（機器）
４０２　ＡＫＥ手段
４０３　パケット化手段
４０４　送信条件の設定管理手段
４０５　パケット受信手段
４０６　暗号化手段
４０７　復号手段
４０８　受信条件の設定管理手段
４０９　フレーム化手段
４１０　フレーム受信手段

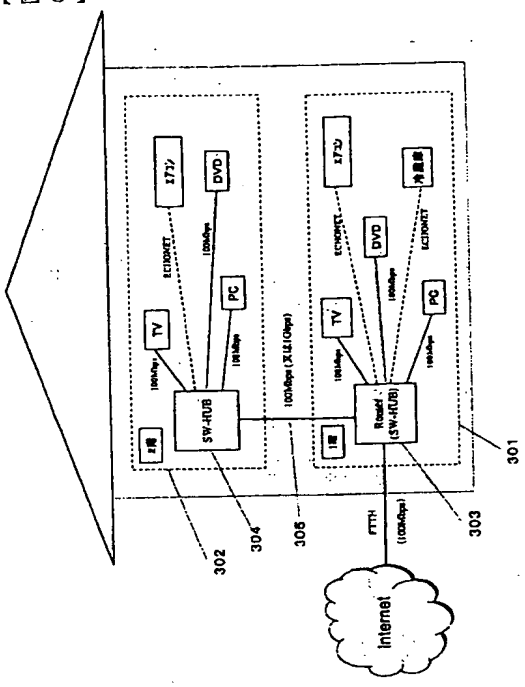
【図１】



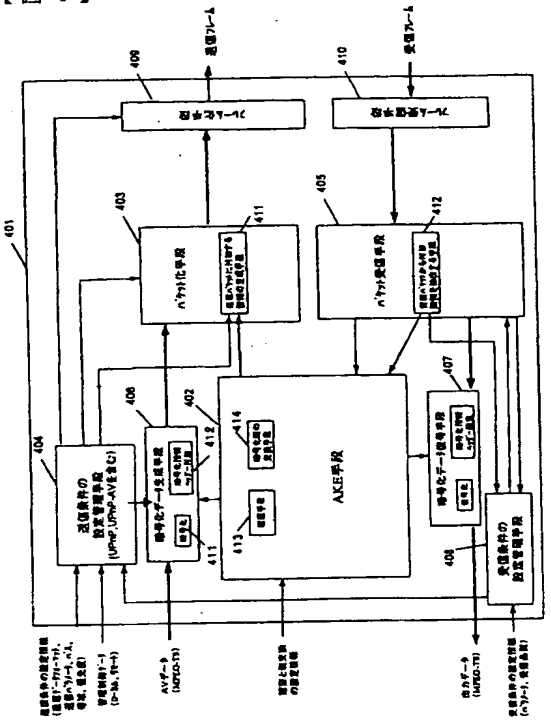
【図２】



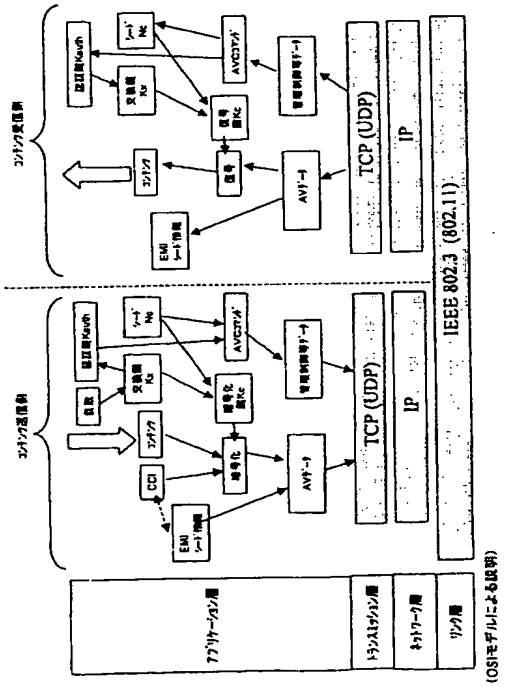
【図３】


SW-HUB
Router (SW-HUB)
TV
DVD
PC
Internet
FTTH
302
303
304
305
301

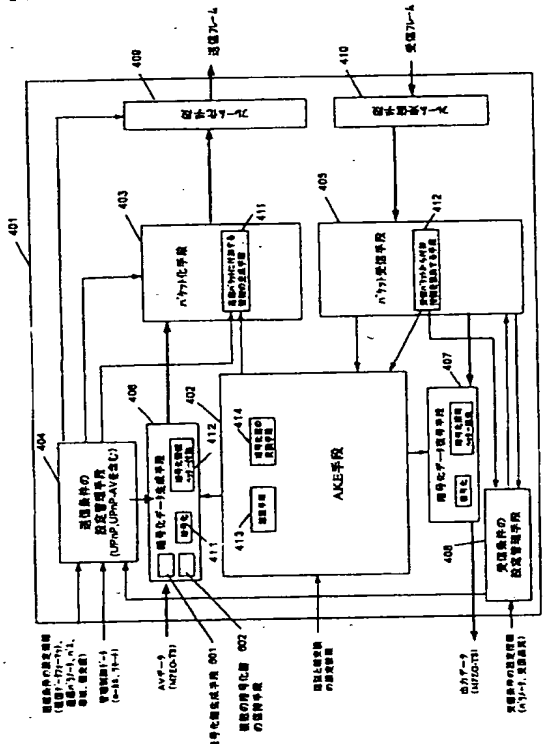
【図４】



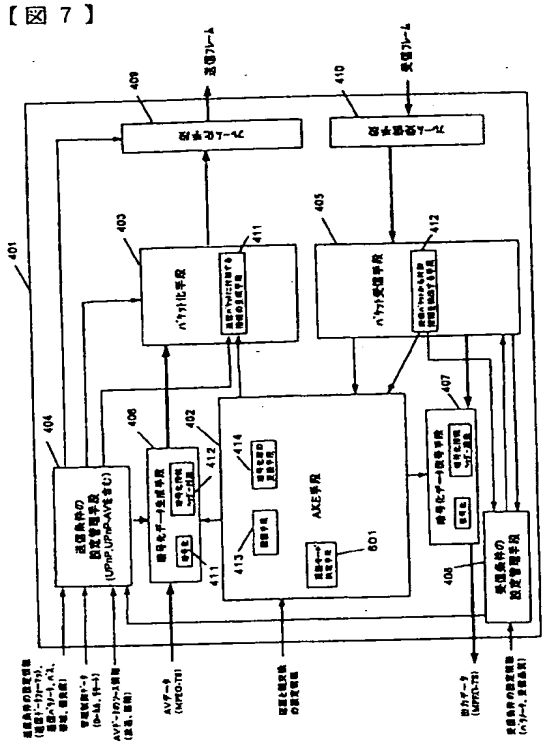
【図５】


TCP (UDP)
IP
IEEE 802.3 (802.11)
(OSIモデルによる説明)

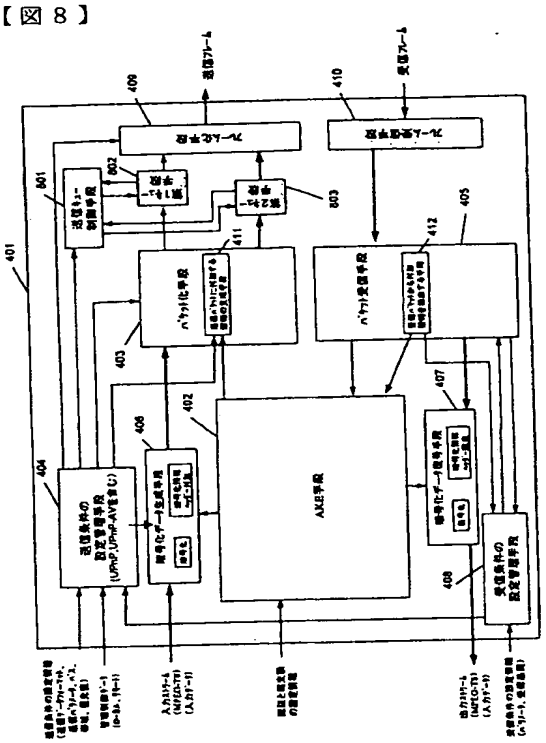
【図６】



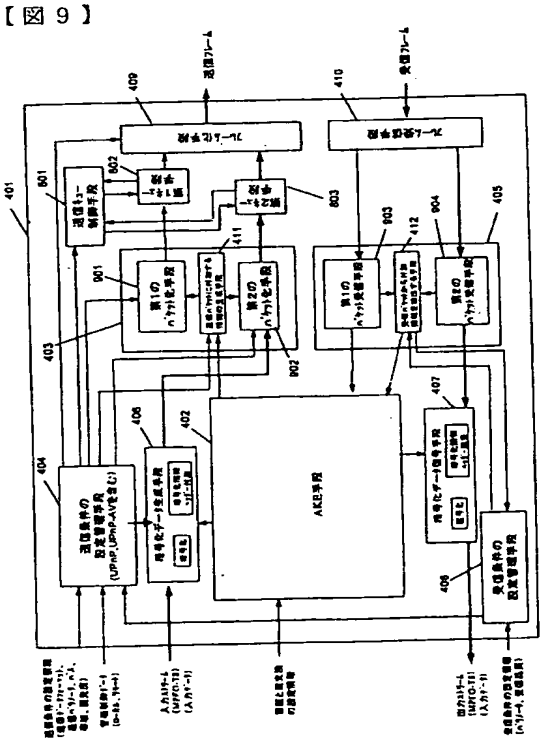
【図７】



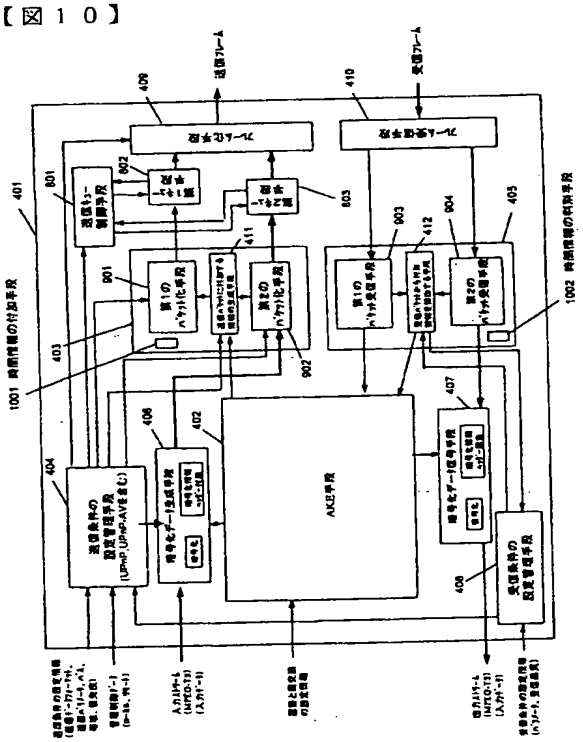
【図８】



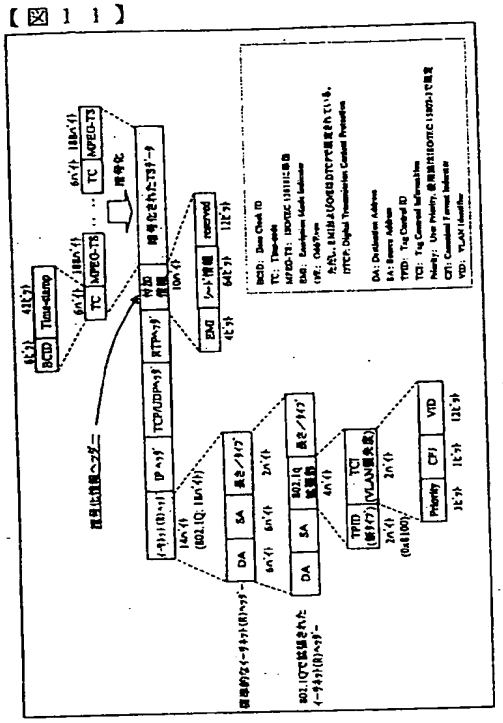
【図９】



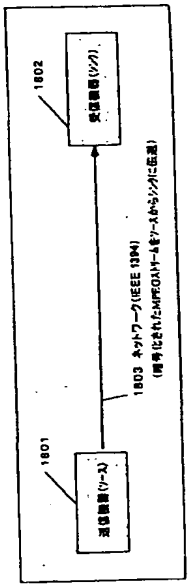
【図１０】



【図１１】



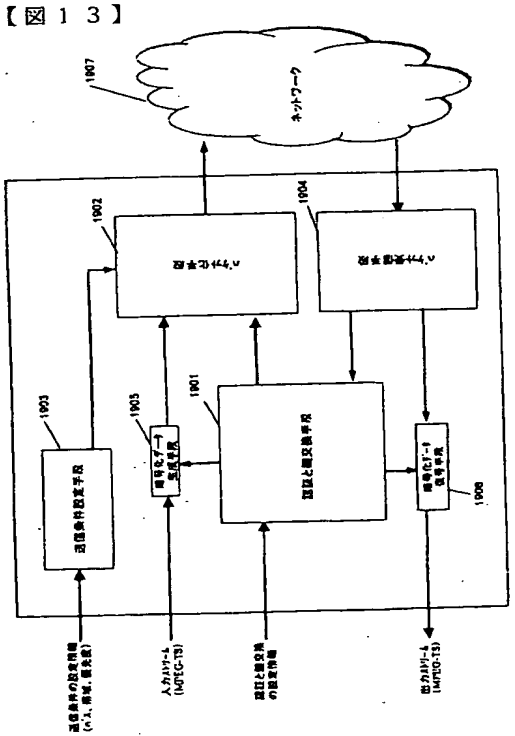
【図１２】



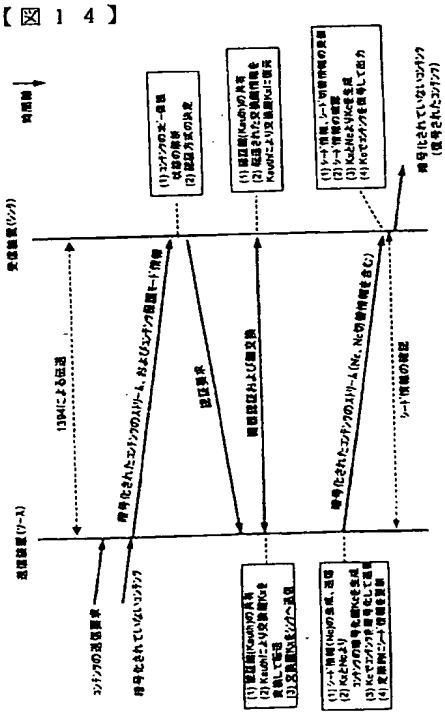
送信機器(ソース)の例	受信機器(シンク)の例	コンテンツ形式における符号化
DVHS	DVHS	MPEG-TS(UDP)方式によるコンテンツ伝送を実施
HDDレコーダ	HDDレコーダ	
1394接続STB	1394接続STB	
1394接続デジタルTV	1394接続デジタルTV	

IEEE 1394におけるCOTCPを用いたMPEG入り一般の伝送

【図１３】

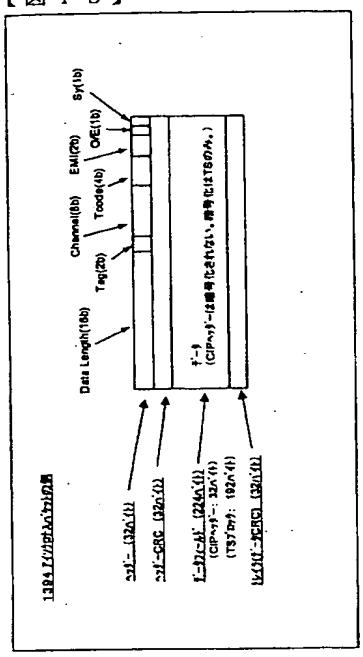


【図１４】



IEEE 1394におけるCOTCPを用いた一般受信ストリーム伝送実施(従来技術)

【図１５】



フロントページの続き

(51)Int.Cl.[7]	F I	テーマコード（参考）
H04N 7/16		

(72)発明者 臼木 直司
大阪府門真市大字門真１００６番地 松下電器産業株式会社内

Ｆターム(参考) 5C025 AA01 AA30 BA27 DA01 DA08
5C063 AB03 AB05 AC10 DA07 DA13
5C064 BA01 BB02 BC16 BC17 BC20 BC22 CA14 CB01 CC04
5J104 AA01 AA12 AA16 EA04 EA16 EA18 JA03 NA02 NA37 PA01
PA05 PA07